Understanding Human Behaviour in Information Security Policy Compliance in a Malaysian Local Authority Organization

Norhayati Sarmoen, Haliyana Khalid (Corresponding author), Siti Zaleha Abd Rasid, Shathees A/L Baskaran & Rohaida Basiruddin

Universiti Teknologi Malaysia, Malaysia

E-mail: haliyana@utm.my

Received: June 11, 2019 Accepted: August 6, 2019 Published: August 16, 2019

doi:10.5296/bms.v10i2.14909 URL: https://doi.org/10.5296/bms.v10i2.14909

Abstract

The utilization of the Information and Communications Technology (ICT), such as the Internet and electronic mail (e-mail) has made communication nowadays easier, faster and has tremendously reduced the usage of paper. However, if the usage of internet is not properly managed, the possibility of confidential information leakage from the inside of the organ behaviour which have led towards the cases of information breach. The factors include the lack of understanding of information policy, the lack of training, poor management support and the insensitivity of the staffs toward safeguarding the information from falling to the wrong hands. Thus, it is suggested that the ICT security protection needs to be robust, secure and reliable so that the use of the internet or social media will not only enhance the communication efficiency, but also to ensure that the information security in an organization is at the most optimum level.ization to other entities outside of the organization may occur. The impacts of this malicious activity are beyond the boundaries and cannot be controlled despite implementing various preventive steps and enforcing various regulations. Previous studies have outlined different factors in influencing information leakages in various organizations. However, none had really identified the severity of the factors up to this day. This research hopes to fill this gap, by focusing on staff in a city council in Johor, Malaysia. This study covers factors related to human.

Keywords: information technology management, information security policy, confidential information, information breach, social media

1. Introduction

The social media platforms such as Facebook, Twitter, Youtube, Blog, WhatsApp and other interaction mediums on the Internet have become essential and have been widely used among many people. These mediums have been used by enablers as a virtual discussion platform, knowledge sharing mediums as well as tools for promotion. The government agencies also benefited from this technology in delivering information faster and more efficient. Nowadays, Facebook is widely considered to be one of the most accessible social networking media among civil servants in Malaysia, even during working hours (MAMPU, 2011). Ishak & Ghani (2015) added that the excessive utilization of Facebook among civil servants may result in the information, whether confidential or non-confidential to be leaked either deliberately or unintentionally. This is mainly due to the ability of Facebook that allows information to be shared amongst colleagues, friends or even families. These civil servants have signed an undertaking of confidentiality as a pledge to show that they understand the circumstances where during the term of employment as a civil servant, any known official information shall not be disclosed, broadcasted or served either verbally, in writing or in any forms without the prior written permission of the parties concerned. By signing this undertaking, civil servants also understand that the attitude of not preserving the security of confidential information is an offense, where disciplinary actions could be taken against them if they disclose the confidential information. Therefore, this paper focuses on understanding the behavioural conducts of Pasir Gudang City Council (MPPG) officers in their official capacities.

As a city council, MPPG is required to comply with the Official Secrets Act 1972 (Act 88). The Act 88, published by the Commissioners of Law Revision, Malaysia, is an act to revise and consolidate the laws related to the protection of official secrets. MPPG also used the Security Instruction as a guideline in implementing the Security Controls in the organization. The book is a guideline and regulation on security controls that must be followed and implemented by all Head of Department in all Ministries, Departments, Statutory Bodies and Government Agencies at Federal and State levels. These rules are formulated to effectively safeguard Malaysia against the issues of confidential information leakage. MPPG is concerned over the needs to rectify its information security and has formulated the information security policy, namely, the MPPG ICT Security Fundamental to ensure that their employees are informed and aware of security risks. The employees are required to understand their responsibility, which is to always safeguard the confidential documents. They are not allowed to disclose any confidential documents to anyone that is irrelevant, except with the authorized permission for the performance of official duties.

This research identified the circumstances that may lead towards information leakage despite the management's initiatives in eliminating the risks of information breach. Human behaviour such as being insensitive towards issues related to information security contributed to an increased profile of information security breaches. An analysis of the critical factors identified human roles as the most vulnerable in contributing towards a systematic risk compared to infrastructures and management system. Social media is a popular medium in this digital age. Therefore, the uncontrolled actions of our fingertips due to human behaviour may lead to the disclosure of confidential information, either unintentionally or deliberately. The observations led to some findings that concluded the elements such as human behaviour, the effectiveness of awareness programme, employees understanding in law and policy and efforts by the management to ensure that their staffs are in compliance with the information security policy. These have become the major factors that may potentially contribute towards confidentiality breach.

2. Research on Information Security Compliance

Information leakage is defined as a breach of the information confidentiality, which may compromise the integrity of the information security. This issue normally originates from the insiders of an organization. According to Molok et al., (2010), cases of information leakage need to be addressed by organizations in order to safeguard their confidential and sensitive information. They covered that the insiders' threats toward the integrity of information security is an organization's major concern, which have become difficult for the organizations to mitigate.

The subject of information security awareness and the appropriate actions to increase the awareness of end users towards the significance of information security have been explored in previous researches. The studies only focused on the organizations' endeavours toward enhancing the information security awareness among employees and the efforts executed by the management team to ensure that the employees are always conscious of the importance of this subject. Kritzinger & Solms (2010) and Talib et al. (2010) agreed that the information security awareness should be a company's greatest emphasis regarding information security. Training and educating the employees is seen as a mandatory part of the organization's information security policies. John M Blythe (2013) has focused on identifying the factors that may influence the information security policy compliance among employees in his research. According to him, the acceptance and the advancement of latest technologies have increased the likelihood of cyber threats to appear. However, researchers nowadays are starting to set their priorities on investigating the behaviours of the users instead of solely studying the user's awareness.

In Malaysia, several media reports have shown that social media is regarded as one of the main factors for a few major cases of leakage of government's top secret confidential information. One example is the case of information leakage regarding The Johore State Government, which involved the amendment of weekend holidays from the initial Saturday and Sunday, to Friday and Saturday (Berita Harian, 18 November 2013). The issues of civil servants' attitudes that underlie the significance of safeguarding the confidential information are seriously concerned by the government. Guidelines and circulars were issued by the government, which emphasizes on the responsibilities of civil servants in maintaining the integrity of information security while using social media on the Internet (Public Service Department Malaysia, 2013). According to Public Service Department Malaysia (2017), the misuse of online social network is one of the cyber threats which may lead towards the leakage of confidential information nowadays. Based on Table 1 shown below, the information leakage cases through network and e-mail recorded a higher percentage compared to other channels.

Table 1. Information Leakage of Media

No	Medium	%
1.	Network (Web, Cloud)	67.4
2.	E-mail	17.2
3.	Printed documents	8.1
4.	Equipment theft/loss	3.0
5.	Removable media (USB pen drive)	2.3
6.	Instant messages (text, voice and video)	2.0
7.	Mobile devices	0.1

Source: Public Service Department Malaysia (2017)

Typical online social networking sites offer a variety set of functions such as status updates, friends' requests, photos and videos uploads, third party applications and links to other websites, making them potential avenues of information leakage (Molok et al., 2011).The social media and big data analytics are indeed fundamentally changing the way we live, work and interact with each other.

Crossler et al. (2013) realized that technological measures alone cannot solely guarantee a total protection of information security in organizations. Therefore, organizations require a considerable amount of efforts to refine the behaviours of information security in employees and end-users as well. As a result, the employees and insiders of an organization play a crucial part in minimizing the risks of an information security system. SAI Global (2008) findings provide general overview of employees' attitude, behaviour and knowledge in relation with the information security. The management of the organization also learned more about their employee's view of information security and how it affects them. Herath & Rao (2009), Bulgurcu et al. (2010), Johnston & Warkentin (2010) and Siponen & Vance (2010) all agreed that human factors inside an organization could be much more threatening than those outside of the organization. This is due to their strong relationship with the organizational information systems and their direct access towards the confidential data and information of the organization.

Thus, this research hopes to identify the root causes of confidential information leakages in the organization in terms of individual attitudes, the effectiveness of implementing awareness programs and level of efforts from the management in order to control and curb the problem. The result from the finding is very important to enhance the awareness and knowledge regarding information security among employees and to cultivate the culture of safeguarding the confidential information in the workplace.

3. Theoretical Framework

In an era where the dependence of information security systems are significantly high, the threats of incidents related to information security that could jeopardize the whole information security system held by organizations are tremendously crucial and critical. Thus, the possible factors which may result in possible threats will be further elaborated and discussed in this section: -

3.1 Behaviour

Safa and Von Solms (2016) suggest that the task of enhancing employees' security awareness and behaviour has always been critical in keeping information security intact.Despite the tremendous development of information security technology, humans, in this case, employees still remain as the weakest link in the information security realm. Siponen and Willison (2009) have conducted several studies which prove that some employees may intentionally abuse the information security systems. This fact is also supported by Richardson (2008), who agreed that although computer hackers and criminals are often headlined in the mainstream media, evidence suggests that more information security incidents occur as a result of internal employee actions. This is due to the fact that employees in this modern era are very accessible to social media. They have an unlimited access to reach the Internet, thus they could effortlessly have an entry to the social media world. Warkentin & Willison (2009) and Workman & Gathegi (2007) agreed to this fact and added that many cases of organizational resources abuse are caused by their own employees, who are the insiders of organizations rather than outsiders. However, Safa & Maple (2016) found out that a lot of information leakage occurred out of unintentional mistakes by employees. Vroom & Von Solms (2004) also indicate that the security incidents caused by insiders are more likely to be accidental rather than intentional. Therefore, in order to ensure that the information security is protected, it is important not only to address the knowledge of users, but also their attitudes and behaviours. A hypothesis that can be drawn from the theories is that there is a relationship between behaviour with the information security.

Hypothesis 1: Behaviour has a significant relationship with the level of protecting information security.

3.2 Awareness Programme

Awareness programs have become key components of security management in effectively tackling the information security problems. These awareness programmes aim to make employees and end-users alert towards the emerging security issues and policies. M.E. Thomson & R. Von Solms (1998) and Rezgui (2008) stated that the implementation of awareness programs is vital in every organisation in order to educate users regarding information security issues. Thus, awareness programs in an organization seek to remind employees regarding the significance of information security through repetitive procedures that support policy and emphasis on practices that will instill awareness in them to comply with the company's policy (Winnipeg, 2008). According to Veseli (2011), an information security awareness program is considered as efficient if the program has the capability to enhance the attitude, behaviour and knowledge of the participants. The programs are also deemed as effective if the awareness programs are able to develop positive changes in terms of security culture in an organization. This fact was argued by Kruger & Kearny (2006), who stated that the implementation of information security awareness programs will never guarantee the instant understanding of all employees regarding their roles in ensuring the maximum security of information. Anderson & Agarwal (2010) and Puhakainen & Siponen (2010) have affirmed that efficient awareness-raising programs are effective in increasing employees' security-related knowledge. This will instill a security-conscious decision making and behaviour amongst them. Talib et al. (2010) stated that education and training are also vital for the enhancement of the security awareness in order to act as a countermeasure to combat the elevating risks and threats exposed to end users. Thus, company should plan on implementing various security-related training and programs for their employees to improve their knowledge regarding information security. From these theories, this study draws a hypothesis, whether if the awareness programme such as training does affect the level of information security or not.

Hypothesis 2: Awareness program has a significant relationship with the level of protecting information security.

3.3 Understanding Law and Policy

Understanding law and policy is one of the most crucial aspects in information security compliance. Baker & Wallace (2007) stated that the purpose of information security policies is to prevent the misuse of information security and to safeguard the information. Doherty & Fulford (2005) agreed that the information security policies nowadays need to be thoroughly reconstructed so that its usefulness in guiding employee's behaviours is crystal clear. Gaskell (2000) classified the existence of law and policy as ad hoc, or commonly known as created with a particular purpose. In an organization, the management will outline a set of instructions to point out the significance of information assets to the employees. This will also aid employees in having a better understanding towards the significance of information security. Von Solms (2004) stated that the policy should provide guidance to employees and this policy acts as a vital instrument to develop information security practices that could ameliorate, or even upgrade the information security management system in an organization. Therefore, an effective information security policy will enable employees to experience a tremendous increment in terms of their awareness regarding the correlation of understanding laws and policies towards improving information security at a more in-depth degree. Winnipeg Audit Department (2008) found out that employees have low level of knowledge in information security policies. Hence, there are still many staffs who do not necessarily know how to fulfil their responsibilities, which may largely increase the risk of confidential information security breach. Therefore, staffs need to have a considerable amount of understanding and knowledge regarding their responsibility in safeguarding the information. From these theories, this study draws a hypothesis, whether if there is a relationship between level of understanding law and policy with the information security or not.

Hypothesis 3: Understanding law and policy has a significant relationship with the level of protecting information security.

3.4 Management Role and Controlling

The management and employees have a legitimate access to the information security system and have been given the authority and responsibility on securing the highly confidential information. Therefore, they must work side by side to prevent incidents such as information security breach or information leakage from occurring. According to the Winnipeg Audit Department assessment (2008), the management have to work closely with the IT management as well as the IT coordinators from other departments in the organization to ensure continuous information security efforts. Molok et. al. (2010), agreed that the capability of others to gain either full control or partial control on users' information in the online service networking has made this medium to require the most strenuous efforts by the management to prevent the cases of information disclosure from happening. This is due to the restriction of the management to monitor and control any information that is deliberately or unintentionally disclosed to the third parties by the employees due to the employees' activities in the online social networking realm. Hu et al. (2012) agreed that the top management plays a vital role in ensuring employee's behavioural compliance with the information security policies. In order to make sure that this is achieved, proactive actions need be taken to ensure that no information are being disclosed to any third parties due to the deliberate or unintentional misconduct by the employees. Despite most of the literatures that were cited here are from outside of the information security context, the fundamental concept in these discussions is relevant, applicable and pertinent to comprehend the roles of top management in controlling and monitoring employees' behaviour regarding the issue of their compliance towards the information security policies. From these theories, this study draws a hypothesis, whether if the management strictly monitor and control the information security from leakage or not.

Hypothesis 4: Management role and controlling has a significant relationship with the level of protecting information security.

3.5 Level of Protecting Information Security

Information security plays an important role in ensuring that all information is protected. Lean-ping & Chien-fatt (2014) stated that the information security consists of technology, process and people elements. All organizations, government agencies or private companies must always be stringent and always keep an eye out for their employees especially in their social media usage. According to MAMPU (2011), Facebook is the social media network that has the most views by civil servants during working hours. In order to enhance the level of protecting the information security in an organisation, factors like behaviours of employees, awareness programme, understanding of law and policy and the management role need to be put into consideration. Bulgurcu et al. (2010) agreed that the necessity of providing the utmost maximum protection towards an organizational information security has been growing in an extremely rapid rate over the past decades. However, Crossler (2013) realized that the total protection of information security in organizations cannot be fully guaranteed by technological measures alone. Therefore, organizations require a considerable amount of efforts to enhance the behaviours of employees and end-users as well towards keeping the integrity of information security intact. Kaur et al. (2018) agreed that the information and data nowadays might not be as secure anymore after passing through precarious networks. This is due to the tremendous increment in terms of the availability of database services on the Internet. According to Baby, A. & Krishnan, H. (2017) the utilization of Internet for communication purposes has rapidly increased. One of the most challenging obstacles for an organisation nowadays is to protect the confidential information and data from falling to the wrong hands. The leakage of confidential information is one of the major threats that could instantly put an organization’s information security in jeopardy. We should always note that if proper actions are taken by the top level (management team) all the way down to the bottom level (employees), the information security management in an organization can be run smoothly. Therefore, the enhancement of employees’ behaviours, proper implementation of awareness programme for the employees and the end-users, high levels of enlightenment regarding laws and policies by the employees and the salient roles of the management team are vital for an organisation’s information security system to operate at its optimum level.

3.6 Conceptual Framework

To strengthen the research, we have developed a conceptual framework model based on the practise of protecting information security in the . The aim of this study is to identify the level of information security policy compliance in the city council and its relationship with human behaviour.

To comply with the Official Secrets Act 1972 and the Arahan Keselamatan, MPPG has provided the information security policy, namely The MPPG ICT Security Fundamental. This policy is provided to ensure a maximum level of information security. The employees are required to understand their responsibilities to always safeguard the confidential information and they are not allowed to disclose any confidential information. However, the policies and guidelines regarding the safety of this information are only understood by employees in the

IT Division and the Administrative Division who are involved. Thus, it makes these policies and guidelines unintelligible to be practiced by MPPG employees in other departments. Therefore, there are variables that are not being researched, which creates a gap towards the objective of MPPG which is to ensure that the level of security of the information is fully guaranteed. This study fills the research gap by providing a useful insight on how behaviour, awareness programme, understanding of law and policy and the roles of management could have a significant relationship with the level of protecting the information security in MPPG. The objectives of this study are also in parallel with the functions and responsibilities of MPPG as Local Authorities in ensuring the maximum information security protection.

This conceptual framework expects to link the components from the current study and to show how these components are related to the level of protecting information security. Figure 1 displays the proposed conceptual framework which was developed based on the study. Based on the review, research hypotheses were developed and a theoretical model is proposed that highlights how behaviour, awareness programme, understanding of law and policy and management role has a significant influence in the level of protecting the information security.

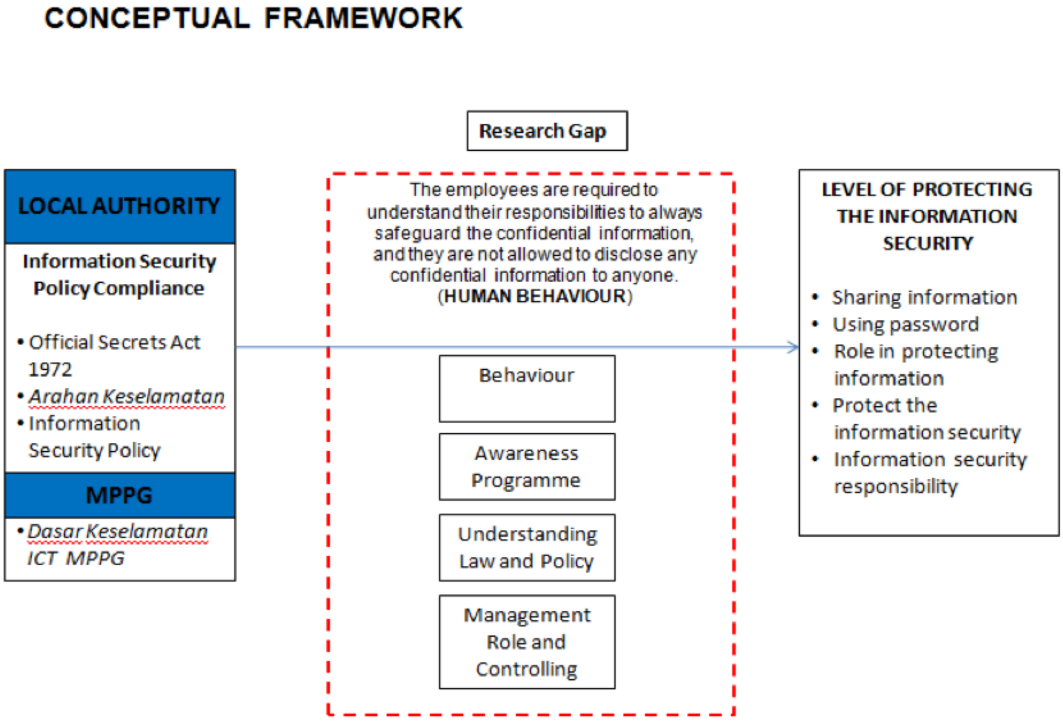
CONCEPTUAL FRAMEWORK
Research Gap
LOCAL AUTHORITY
Information Security Policy Compliance
• Official Secrets Act 1972
• Arahan Keselamatan
• Information Security Policy
MPPG
• Dasar Keselamatan ICT MPPG
The employees are required to understand their responsibilities to always safeguard the confidential information, and they are not allowed to disclose any confidential information to anyone. (HUMAN BEHAVIOUR)
Behaviour
Awareness Programme
Understanding Law and Policy
Management Role and Controlling
LEVEL OF PROTECTING THE INFORMATION SECURITY
• Sharing information
• Using password
• Role in protecting information
• Protect the information security
• Information security responsibility

Figure 1. Conceptual Framework Model of the research gap from the previous research

The above elements which are behaviour, awareness programme, the understanding of law and policy and management role can significantly influence individuals' behavioural intentions towards their compliance with the information security policies.

3.7 Hypothesis Development

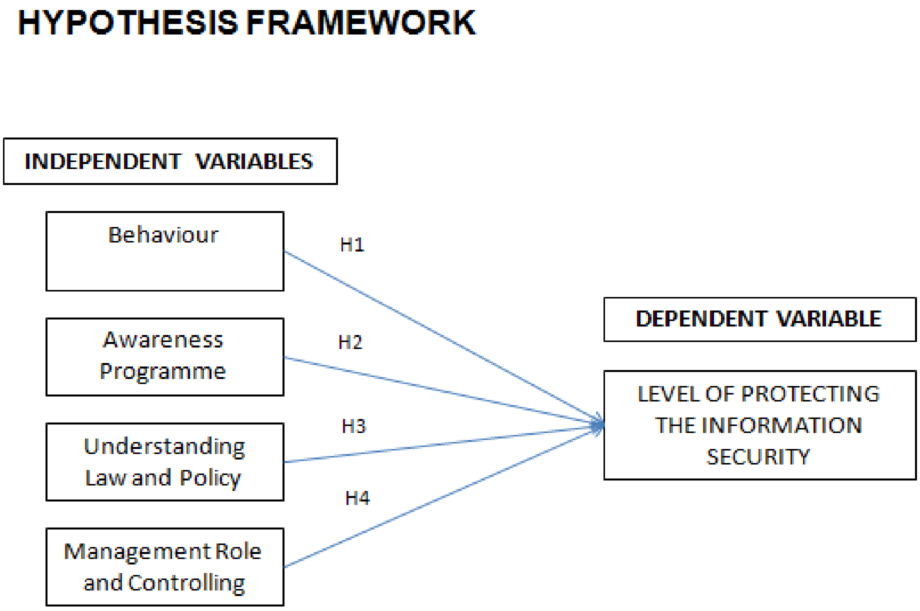
HYPOTHESIS FRAMEWORK
INDEPENDENT VARIABLES
Behaviour
Awareness Programme
Understanding Law and Policy
Management Role and Controlling
H1
H2
H3
H4
DEPENDENT VARIABLE
LEVEL OF PROTECTING THE INFORMATION SECURITY

Figure 2. Hypothesis Development

The research framework for this study identified four independent variables that could lead to the issues of information leakages, which are behaviour, awareness programmes, understanding of law and policy and management role and controlling (see Figure 2). These independent variables represent the factors that have a significant relationship with the level of protecting the information security, which is the dependent variable.

Therefore, there are four hypotheses that have been established to be tested in this study:

H1: Behaviour has a significant relationship with the level of protecting information security.

H2: Awareness program has a significant relationship with the level of protecting information security.

H3: Understanding of law and policy has a significant relationship with the level of protecting information security.

H4: Management role and controlling has a significant relationship with the level of protecting information security.

4. Research Methodology

This research was conducted by distributing the questionnaires to the respondents. The questionnaire is used as an instrument to analyse the behaviour, the effectiveness of awareness programmes, level of understanding on the law and policy, and the enforcement by the management as the study variables in assessing their impacts towards the level of information security. A total of 242 questionnaires were distributed to the city council management and supporting staffs. However, only 233 questionnaires were returned with completed answers. Descriptive analysis is used to assist in describing, presenting and summarizing the respondents' demographics profile. Apart from the survey, the secondary data were also acquired from the previous studies related to the topic. The data were analyzed by using the Descriptive analysis, Cronbach Alpha Reliability Test and Pearson Correlation Analysis.

5. Results and Analysis

In this section, we explain results from data analysis.

5.1 Reliability and Normality Analysis

Table 2 below shows the instrument reliabilities for actual data and the combination of all independent variables, using Cronbach's Alpha Reliability Test. The test has a result of 0.911. This indicates that there is a good internal consistency of all 28 items in the scale.

Table 2. Cronbach's Alpha Reliability Test Result (All Independent Variables)

Variables	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
Independent variables	0.911	0.913	28

The Cronbach's Alpha value in all independent variables as presented in Table 3 and 4 was 0.898, with 23 numbers of items, while the Cronbach's Alpha value for dependent variable was 0.730, with 5 numbers of items. According to Zinbarg (2005) this indicates that there is good internal consistency of all the 28 items in the scale because the Alpha Coefficient Range is greater than 0.7.

Table 3. Cronbach's Alpha Reliability Test Result (All Independent Variables)

Variables	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
Independent variables	0.898	0.900	23
Dependent Variable	0.730	0.724	5

Table 4. Cronbach's Alpha Reliability Test Result (Independent Variable)

Variables	Number of Items	Cronbach's Alpha (n = 233)
Human Behaviour	6	.824
Awareness Programme	6	.728
Law and Policy	5	.802
Management Role	6	.823
Level of Protecting the Information Security	5	.826

5.2 Pearson Correlation Analysis

Pearson Correlation Analysis is used to measure how correlated and connected the variables are. Hence, a Pearson Correlation Analysis was computed in this study to assess the relationship between types of search, sequence of search, credibility of information and extent of search towards purchasing decisions.

In Table 5, all variables have coefficients of higher than 0.4. After analysing the data using Pearson Correlation Analysis, this signifies that the correlation of these variables with the level of information security is moderate or medium (Hopkins, 2002).

Table 5. All Variable Correlation Coefficient

Variables	Coefficient, *r*	Significance level, *p*
Human Behaviour	0.500	0.000
Awareness Programme	0.549	0.000
Law and Policy	0.439	0.000
Role of Management	0.484	0.000

All the hypotheses were tested using Pearson correlation coefficient to measure the correlation between the variables. The results showed a positive correlation between the variables and the level of protecting the information security.

Table 5 shows the correlation results and Table 6 shows the summary of Pearson Correlation Analysis results in detail which have been conducted for this study. There is a strongly positive relationship between the two variables, r=.628, n=233, p<.01, with high levels of behaviour associated with higher levels of information security for the respondents. Since all of the variables are positively correlated with the level of protecting information security, all hypotheses tested are accepted (see Table 7).

Table 6. Correlations Results

		Human Behaviour	Awareness Programme	Law And Policy	Management Role	Level of Information Security
Human Behaviour	Pearson Correlation	1	.436**	.504**	.421**	.500**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	233	233	233	233	233
Awareness Programme	Pearson Correlation	.436**	1	.439**	.468**	.549**
	Sig. (2-tailed)	.000		.000	.000	.000
	N	233	233	233	233	233
Law And Policy	Pearson Correlation	.504**	.439**	1	.616**	.439**
	Sig. (2-tailed)	.000	.000		.000	.000
	N	233	233	233	233	233
Management Role	Pearson Correlation	.421**	.468**	.616**	1	.484**
	Sig. (2-tailed)	.000	.000	.000		.000
	N	233	233	233	233	233
Level of Information Security	Pearson Correlation	.500**	.549**	.439**	.484**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	233	233	233	233	233

Table 7. Summary of Pearson Correlation Analysis Results

No.	Hypotheses	Value	Remarks
H_1	Behaviour has a significant relationship with the level of protecting information security.	*r*=.500, *p*<.01	Accepted
H_2	Awareness program has a significant relationship with the level of protecting information security.	*r*=.549, *p*>.01	Accepted
H_3	Understanding law and policy has a significant relationship with the level of protecting information security.	*r*=.439, *p*<.01	Accepted
H_4	Management role and controlling has a significant relationship with the level of protecting information security.	*r*=.484, *p*<.01	Accepted

6. Discussions

This research aims to understand the human behaviour which affects the employees' information security policy compliance in the organization. The objective of this research is to explore the relationship between behaviour and the level of safeguarding the information security in an organization. The findings of this research have discovered that there is a significant relationship between behaviour, awareness programme, the understanding of law and policy and the management role with the level of protecting the information security within the organization. The objective of this research is achieved as follows:-

The factors of human behaviour that influence the level of protecting information security in MPPG were the effectiveness of awareness program, human behaviour, understanding of law and policy and the management role. These factors were identified based on the results from the descriptive analysis. Therefore, the roles of the management and the employees in safeguarding the whole information security need to be emphasized, especially when the risks of cyber threats are extremely high.

The most contributing factors of human behaviour that can influence the level of protecting the information security in MPPG are the effectiveness of awareness programme and the human behaviour itself. These factors were identified based on the results from Pearson Correlation analysis. Since most of the impacts are towards security practice-care behaviour, the online file sharing and data protection are very important to be considered.

There is a moderately positive relationship between human behaviour and the level of information security in MPPG which indicates that the organization's efforts, such as implementing effective awareness programme are significant enough in controlling the level of information security. Employees who do not comply with information security policy guidelines will bring serious risks toward their organizations. According to Kankanhalli et al. (2003), the security guidelines are provided to all employees so that they can become even more effective to prevent any possibilities of severe damages towards an organization's information assets. This research shows that employees' behaviours play an important role in avoiding vulnerabilities and has a significant relationship with the level of protecting information security in MPPG.

7. Conclusion

In order to ensure the maximum level of information security, organizations need to cultivate the culture of "security conscious workforce" from the top level (management team) to the bottom level (employees). The organization also needs to provide information security policies that are clear and understandable to all employees at all levels to prevent the misuse of information security and to safeguard the information.

Acknowledgement

The research is financed by UTM Research Grant, No Q. K130000.2763.03K15

References

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. MIS quarterly, 34(3), 613-643. https://doi.org/10.2307/25750694

Baby, A., & Krishnan, H. (2017). A Literature Survey on Data Leak Detection And Prevention Methods. *International Journal*, *8*(5), 2416-2418.

Baker, W. H., & Wallace, L. (2007). Is information security under control? Investigating quality in information security management. *IEEE Security & Privacy*, *5*(1). https://doi.org/10.1109/MSP.2007.11

Berita, H. (2013). Tak Wajar Bocor Maklumat Dokumen Rasmi. http://www.bharian.com.my

Blythe, J. (2013). Cyber security in the workplace: Understanding and promoting behaviour change. *Proceedings of CHItaly 2013 Doctoral Consortium*, *1065*, 92-101. https://10.1016/j.amepre.2016.06.015

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly, 34*(3), 523-548. https://doi.org/10.2307/25750690

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & security, 32*, 90-101. https://doi.org/10.1016/j.cose.2012.09.010

Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: an exploratory analysis. *Information resources management journal, 18*(4), 21. https://doi.org/ 10.4018/irmj.2005100102

Gaskell, G. (2000). Simplifying the onerous task of writing security policies. In Proceedings of the First Australian Information Security Management Workshop.

Global, S. A. I. (2008). SAI Global Information Security Awareness Survey 2008.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165. https://doi.org/10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125. https://doi.org/10.1057/ejis.2009.6

Hopkins, K. M. (2002). Organizational citizenship in social service agencies. *Administration in Social Work, 26*(2), 1–15. https://doi.org/10.1300/J147v26n02_01

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Ishak, M. S. B., & Ghani, J. B. A. (2015). Pengurusan Privasi Facebook Penjawat Awam: Pengaruh Intensiti Penggunaan, Kemahiran Swaawas Dan Orientasi Privasi Organisasi. *Jurnal Komunikasi, Malaysian Journal of Communication, 31*(2).

ISO/IEC (2005). Information Technology- Security techniques: Code of practice for information security management, ISO/IEC 17799:2005(E).

Jabatan Perkhidmatan Awam (2013), Surat pekeliling : Tanggungjawab Pegawai Awam Dalam Memelihara Integriti Perkhidmatan Awam Semasa Menggunakan Kemudahan Media Sosial Di Internet

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly,* 549-566. https://doi.org/ 10.2307/25750691

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International journal of information management,* *23*(2), 139-154. https://doi.org/10.1016/S0268-4012(02)00105-6

Kaur, K., Gupta, I., & Singh, A. K. (2018). Data leakage prevention: e-mail protection via gateway. In *Journal of Physics: Conference Series* (Vol. 933, No. 1, p. 012013). IOP Publishing. https://doi.org/ 10.1088/1742-6596/933/1/012013

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security, 29*(8), 840-847. https://doi.org/10.1016/j.cose.2010.08.001

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & security, 25*(4), 289-296. https://doi.org/10.1016/j.cose.2006.02.008

MAMPU, Public Sector CIO Convex Report 2016, Digital Government Towards Digital Citizens

Molok, N. N. A., Ahmad, A., & Chang, S. (2010). Understanding the factors of information leakage through online social networking to safeguard organizational information. In *Proceedings of the 21st Australasian Conference on Information Systems (ACIS).* https://aisel.aisnet.org/acis2010/62

Molok, N. N. A., Ahmad, A., & Chang, S. (2011). Information leakage through online social networking: Opening the doorway for advanced persistence threats. *Journal of the Australian Institute of Professional Intelligence Officers, 19*(2), 38.

Official Secrets Act 1972 (Act 88).

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *Mis Quarterly*, 757-778. https://doi.org/ 10.2307/25750704

Safa, N. S., & Maple, C. (2016). Human errors in the information security realm–and how to fix them. *Computer Fraud & Security, 2016*(9), 17-20. https://doi.org/10.1016/S1361-3723(16)30073-2

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442-451. https://doi.org/10.1016/j.chb.2015.12.037

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502. https://doi.org/ 10.2307/25750688

Talib, S., Clarke, N. L., & Furnell, S. M. (2010, February). An analysis of information security awareness within home and work environments. In Availability, Reliability, and Security, 2010. ARES'10 International Conference on (pp. 196-203). *IEEE.* https://doi.org/10.1109/ARES.2010.27

Thomson M.E and R. Von Solms (1998), Information Security Awareness: Educating Your Users Effectively. *Information Management & Computer Security, 6*(4), 167-173. https://doi.org/10.1108/09685229810227649

Veseli, I. (2011). Measuring the Effectiveness of Information Security Awareness Program (Master's thesis).

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198. https://doi.org/10.1016/j.cose.2004.01.012

Von Solms, R., & Von Solms, B. (2004). From policies to culture. *Computers & security, 23*(4), 275-279. https://doi.org/10.1016/j.cose.2004.01.013

Von Solms, R. (1998). Information security management (3): The code of practice for information security management (BS 7799). *Information Management & Computer Security, 6*(5), 224-225. https://doi.org/10.1108/09685229810240158

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18*(2), 101-105. https://doi.org/10.1057/ejis.2009.12

Winnipeg (2008), Assessment of Information Security Awareness: Information Security Awareness-Final Report, Winnipeg, Audit Department. https://doi.org/10.1016/j.procs.2015.12.151

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the Association for Information Science and Technology, 58*(2), 212-222. https://doi.org/10.1002/asi.20474

Zinbarg, M. (2005). Research methods. Pearson Publishers. www. ijcbss. org ISSN, 2312, 59861.

Copyright